

# MINIMAL RAMIFICATION AND THE INVERSE GALOIS PROBLEM OVER THE RATIONAL FUNCTION FIELD $\mathbb{F}_p(t)$

MEGHAN DEWITT

**ABSTRACT.** The inverse Galois problem is concerned with finding a Galois extension of a field  $K$  with given Galois group. In this paper we consider the particular case where the base field is  $K = \mathbb{F}_p(t)$ . We give a conjectural formula for the minimal number of primes, both finite and infinite, ramified in  $G$ -extensions of  $K$ , and give theoretical and computational proofs for many cases of this conjecture.

## 1. INTRODUCTION

In 1892 Hilbert proposed the first systematic approach to solving the question of which finite groups occur as Galois groups over the rational numbers  $\mathbb{Q}$ , using his Irreducibility Theorem to consider the problem over  $\mathbb{Q}(t)$  [?, Page v]. Since his work, the question of which finite groups occur as Galois groups over  $\mathbb{Q}$ , then later over any field  $K$ , has been studied extensively.

What types of restrictions can we place on the field extension for a given group  $G$ ? Can we produce a  $G$ -extension that is ramified at a specific prime, or unramified outside of a set of primes? We consider the case, for a fixed finite group  $G$  and global field  $K$ , of finding the minimal number of primes that will ramify in any  $G$ -extension of  $K$ .

Let  $K$  be a global field, and define

$$\text{Ram}_K(G) := \min_{\text{Gal}(L/K) \cong G} \#\{\text{places that ramify in } L/K\}.$$

Let  $d(G)$  denote the minimum number of generators for the group  $G$ . For completeness, we set  $d(\{1\}) = 0$ . Also, we define  $p(G)$  to be the normal subgroup generated by the elements of  $p$ -power order.

Work of Boston and Markin [?] explored this question in the case where  $K = \mathbb{Q}$ , giving the expected minimal number of ramified primes as  $d(G^{ab})$ . Harbater [?] and Raynaud [?] proved Abhyankar's Conjecture, which covers the same situation for  $K = \overline{\mathbb{F}_p}(t)$ , giving the minimal number of ramified primes as  $d(G/p(G)) + 1$ . Grothendieck explored the same issue with his work on the fundamental group of the punctured projective line [?, ?].

In the following, we consider the case where  $K = \mathbb{F}_p(t)$ . Further, we restrict attention to geometric extensions, meaning we do not allow any extension of the field of constants, which gives us a trivial lower bound  $\text{Ram}_K(G) \geq 1$  for any non-trivial group  $G$  [?, Page 106]. In addition, we know that class field theory will provide us with a better lower bound; see Theorem 2.3, Theorem 2.6, and Corollary 2.7 contained herein.

---

*Date:* October 31, 2014.

*Key words and phrases.* Function Fields, Ramification, Inverse Galois.

Based on this related work and numerous families of examples, we have the following conjecture:

**Conjecture 1.1** (Restricted inverse Galois problem over Function Fields). *If  $G$  is a non-trivial finite group then there exists a  $G$ -extension of  $\mathbb{F}_p(t)$  and*

$$\text{Ram}_{\mathbb{F}_p(t)}(G) = \begin{cases} d+1 & \text{if } p \mid |G^{ab}| \\ \max(d, 1) & \text{if } p \nmid |G^{ab}| \end{cases}$$

where  $d = d((G/p(G))^{ab})$ .

We provide proofs for abelian group, groups of prime power order, and nilpotent groups, as well as several other families of examples.

## 2. BASIC RESULTS

We begin with the basic building blocks, namely abelian groups and  $p$ -groups. When tackling the abelian groups, it is useful to have a function field analogue of the Kronecker-Weber Theorem. To do this, we turn to Carlitz-Hayes Theory [?].

For each polynomial  $M \in \mathbb{F}_p[t]$  we define the Carlitz polynomial  $[M](x)$  with coefficients in  $\mathbb{F}_p[t]$  recursively:

$$\begin{aligned} [1](x) &= x \\ [t](x) &= x^p + tx \\ [t^n](x) &= [t]([t^{n-1}](x)) \\ [c_n t^n + \cdots + c_1 t + c_0](x) &= c_n [t^n](x) + \cdots + c_1 [t](x) + c_0 [1](x). \end{aligned}$$

In addition, we use a similar definition with  $1/t$  in place of  $t$ :

$$\left[\frac{1}{t}\right](x) = x^p + \frac{x}{t}.$$

Let  $K$  be a field extension of  $\mathbb{F}_p(t)$ . We make  $K$  into an  $\mathbb{F}_p[t]$ -module by letting  $\mathbb{F}_p[t]$  act on  $K$  through the Carlitz polynomials:

$$M \cdot \alpha = [M](\alpha).$$

Define

$$\Lambda_M = \{\lambda \in \overline{\mathbb{F}_p(t)} \mid [M](\lambda) = 0\}.$$

Then  $\mathbb{F}_p(t, \Lambda_M)/\mathbb{F}_p(t)$  is an abelian extension called a cyclotomic function field extension. Note that  $\Lambda_M$  is a free  $\mathbb{F}_p[t]/M$ -module of rank 1. Choose  $\sigma \in \text{Gal}(\mathbb{F}_p(t, \Lambda_M)/\mathbb{F}_p(t))$  and let  $\lambda$  be a generator of  $\Lambda_M$ . Then  $\sigma$  acts as  $A$  on  $\lambda$  for some  $A \in (\mathbb{F}_p[t]/M)^\times$ , and  $\sigma$  acts by the Carlitz action  $[A]$  on all the elements of  $\Lambda_M$ . We write  $A$  as  $A_\sigma$ . Then define

$$\Phi(M) = |(\mathbb{F}_p[t]/M)^\times|.$$

**THEOREM 2.1** (Carlitz). *The map  $\sigma \mapsto A_\sigma$  is then an isomorphism*

$$\text{Gal}(\mathbb{F}_p(t, \Lambda_M)/\mathbb{F}_p(t)) \longrightarrow (\mathbb{F}_p[t]/M)^\times.$$

THEOREM 2.2 (Hayes). *Every finite abelian extension of  $\mathbb{F}_p(t)$  lies in*

$$\mathbb{F}_{p^s}(t, \Lambda_M, \Lambda_{1/t^n})$$

*for some  $s \geq 1$ ,  $n \geq 1$ , and  $M \in \mathbb{F}_p[t]$ , where  $\Lambda_{1/t^n}$  is the set of roots of the Carlitz polynomial  $[1/t^n](x)$  built with  $1/t$  in place of  $t$ .*

**2.1.  $p$ -groups.** We first consider the case where  $G$  is an abelian  $p$ -group.

THEOREM 2.3. *If  $G$  is a nontrivial finite abelian  $p$ -group, then Conjecture 1.1 holds. Namely, there exists a  $G$ -extension of  $\mathbb{F}_p(t)$  ramified at exactly 1 prime (counting the infinite prime), and there are no unramified  $G$ -extensions.*

*Proof.* As we are only considering the geometric case, minimality is immediate. Note that

$$\begin{aligned} H_{n,p} &= \text{Gal}(\mathbb{F}_p(t, \Lambda_{1/t^{n+1}}) / \mathbb{F}_p(t)) \\ &\cong (\mathbb{F}_p[1/t] / (1/t^{n+1}))^\times \\ &\cong \{1 + a_1 + \cdots + a_n t^n \mid a_i \in \mathbb{F}_p\} \times \mathbb{F}_p^\times \end{aligned}$$

by Hayes [?]. Then by Lemma 4.4 of Koch [?], we have that

$$H_p = \varprojlim H_{n,p} / \mathbb{F}_p^\times$$

where  $H_p$  is the Galois group of the maximal  $p$ -extension of  $\mathbb{F}_p(t)$ , is a free abelian pro- $p$  group on countably many generators. Note that by construction only the infinite prime ramifies as ramification of finite primes is contained in an extension of the form  $\mathbb{F}_p(t, \Lambda_M)$  for abelian groups. Then every finite abelian  $p$ -group appears as a quotient of this group.  $\square$

To understand general  $p$ -extensions, let  $\bar{k}_p$  be the maximal  $p$ -extension of a field  $k$  ramified only at infinity. Denote  $G_{k,p} = \text{Gal}(\bar{k}_p/k)$ .

THEOREM 2.4. [?, p. 93, Thm 9.1] *If  $k$  is a field of characteristic  $p$ , then  $G_{k,p}$  is a free pro- $p$  group with generator rank*

$$\dim_{\mathbb{F}_p} k^+ / \mathfrak{p}(k^+)$$

*where we have put*

$$\mathfrak{p}(x) = x^p - x.$$

THEOREM 2.5. *If  $G$  is a nontrivial finite  $p$ -group, then Conjecture 1.1 holds. Namely, there exists a  $G$ -extension of  $\mathbb{F}_p(t)$  ramified at exactly 1 prime (counting the infinite prime), and there are no unramified  $G$ -extensions.*

*Proof.* Consider the extension  $\bar{k}_p/k$  defined above where  $k = \mathbb{F}_p(t)$ . Since every  $p$ -extension has a nontrivial abelian subextension, by Theorem 2.3 and Carlitz-Hayes Theory we know this subextension must be contained in a field of the form

$$\mathbb{F}_{p^s}(t, \Lambda_{1/t^n}) / \mathbb{F}_p(t)$$

which is only ramified at infinity.

Conversely,  $\bar{k}_p/k$  cannot be ramified at a prime other than the prime at infinity, by its Artin-Schreier construction. Thus  $G_{k,p}$  is only ramified at the prime at infinity. Since it is

free pro- $p$  on countably many generators by Theorem 2.4, every finite  $p$ -group occurs as a subextension. □

**2.2. Abelian groups.** We now turn our attention to abelian groups:

**THEOREM 2.6.** *If  $G$  is a nontrivial finite abelian group, then Conjecture 1.1 holds.*

*Proof.* Write  $d = d(G/p(G))$ .

First, we consider the case where  $|G|$  is prime to  $p$ . Then write

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_d\mathbb{Z}.$$

Then for each  $i$  we can choose a nonzero irreducible  $M_i \in \mathbb{F}_p[t]$  such that

$$\Phi(M_i) \equiv 0 \pmod{(p-1)n_i}$$

and the  $M_i$  are distinct and nonassociate. It follows that  $\mathbb{Z}/n_i\mathbb{Z}$  is isomorphic to a quotient of  $(\mathbb{F}_p[t]/M_i)^\times$ . Thus, by taking a direct product,  $G$  is isomorphic to  $\text{Gal}(K/\mathbb{F}_p(t))$  where  $K$  is a subfield of the compositum of the  $M_i$ th cyclotomic function fields

$$\mathbb{F}_p(t, \Lambda_{M_i})/\mathbb{F}_p(t)$$

for  $1 \leq i \leq d$ .

Note that since each  $M_i$  is irreducible and pairwise nonassociate,  $K$  is ramified at exactly  $d$  finite primes. Also, since by a Theorem 3.2 in [?]  $e_\infty = p-1$  in the full  $M_i$ th cyclotomic field, by our choice of  $M_i$ ,  $K$  is a subfield of the compositum of the real portion of the  $M_i$ th cyclotomic fields (meaning the portion not ramified at the infinite prime). Thus, there are  $d$  primes ramified.

Conversely, suppose  $K/\mathbb{F}_p(t)$  is a geometric extension with Galois group  $G$  and is ramified at the finite primes  $\pi_1, \dots, \pi_k$  and possibly at the infinite prime, and no others. By Carlitz-Hayes,  $K$  is a subfield of a cyclotomic function field  $L = \mathbb{F}_p(t, \Lambda_M, \Lambda_{1/t^n})$  for some  $n \geq 1$  and

$$M = \pi_1^{r_1} \cdots \pi_k^{r_k}.$$

If  $K$  is tamely ramified at infinity, then  $K$  is a subfield of  $L^+ = \mathbb{F}_p(t, \Lambda_M)$ . Then  $G$  is isomorphic to a quotient of

$$(\mathbb{F}_p[t]/\pi_1^{r_1})^\times \times \cdots \times (\mathbb{F}_p[t]/\pi_k^{r_k})^\times$$

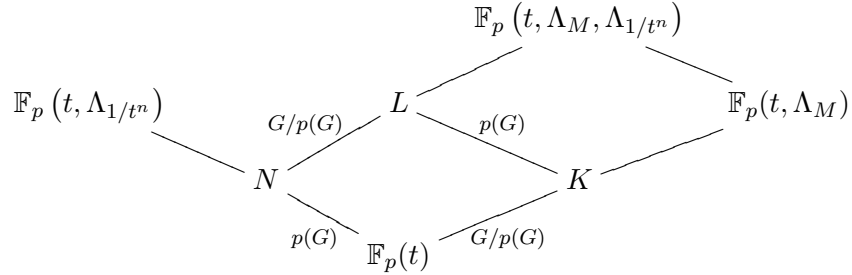
and hence has less than or equal to  $k$  generators.

If  $K$  is not tamely ramified at infinity, then let  $K^+ = K \cap L^+$ , and  $G^+ = \text{Gal}(K^+/\mathbb{F}_p(t))$ . Then, as above,  $G^+$  has at most  $k$  generators. Thus  $G$  has less than or equal to  $k$  generators.

Now, suppose  $|G|$  is not prime to  $p$  (See Figure 1). We obtain the desired extension by using the above for the prime-to- $p$  part and then using Theorem 2.5 to obtain the  $p$ -portion. Since  $G$  is abelian, we can then realize  $G$  by taking the compositum of these two fields.

Conversely, suppose we have a geometric  $G$ -extension  $K/\mathbb{F}_p(t)$ . By the above, the prime-to- $p$  part has at least  $d$  ramified primes. Thus it remains to show that every abelian  $p$ -extension of  $\mathbb{F}_p(t)$  is ramified at the infinite prime. However, this follows from Carlitz-Hayes theory and the fact that the degree of cyclotomic extensions of the form  $\mathbb{F}_p(t, \Lambda_M)/\mathbb{F}_p(t)$  are always prime-to- $p$ . □

FIGURE 1. Breakdown of an Abelian Extension



Then we have also established the following:

COROLLARY 2.7.

$$\text{Ram}_{\mathbb{F}_p(t)}(G) \geq \begin{cases} d+1 & \text{if } p \mid |G^{ab}| \\ \max(d, 1) & \text{if } p \nmid |G^{ab}| \end{cases}$$

holds for any nontrivial finite group  $G$ .

### 3. SEMIABELIAN GROUPS

Theorem 2.5 established that Conjecture 1.1 holds for  $p$ -groups; we now consider  $l$ -groups, where  $l$  is a prime different from  $p$ . Specifically, we consider the case of semiabelian  $l$ -groups, which leads to a more general result. The following are from [?]:

DEFINITION 3.1. Let  $G, H$  be finite groups. We define the wreath product  $H \wr G$  of  $H$  with  $G$  to be the semidirect product  $H^{|G|} \rtimes G$ , where  $H^{|G|}$  is the direct product of  $|G|$  copies of  $H$ , with  $G$  acting on  $H^{|G|}$  by permuting the copies of  $H$  as in the regular (Cayley) representation of  $G$ .

We define the wreath length of a group  $G$  to be the smallest positive integer  $r$  such that there are finite cyclic groups  $C_1, \dots, C_r$  and an epimorphism

$$C_1 \wr (C_2 \wr (\dots \wr C_r) \dots) \twoheadrightarrow G,$$

if such a number exists, and denote it  $wl(G)$ .

DEFINITION 3.2. A finite group  $G$  is called semiabelian if there exists a sequence

$$G_0 = \{1\}, G_1, \dots, G_n = G$$

such that  $G_i$  is a homomorphic image of a semidirect product  $A_i \rtimes G_{i-1}$  with  $A_i$  abelian,  $i = 1, \dots, n$ .

PROPOSITION 3.3. [?] For any prime  $l$ , the smallest family containing all cyclic  $l$ -groups that is closed under homomorphic images, direct products, and wreath products is the family of semiabelian  $l$ -groups. Furthermore, for the elements of this family the wreath length is defined and is exactly  $d(G)$ .

LEMMA 3.4. [?] *Let  $K$  be a global field. Let  $\mathfrak{a}_1, \dots, \mathfrak{a}_s \in \mathcal{I}_{\mathfrak{p}}$  such that their images in  $\mathcal{Cl}_K^{(l)}$  form a minimal set of generators. Let  $l_{m_i}$  be the order of  $\overline{\mathfrak{a}_i}$  and  $\mathfrak{a}_i^{l_{m_i}} = (a_i) \in \mathcal{P}_{\mathfrak{p}}$ . Let  $K'' = K(\zeta_{l^m}, \sqrt[l^m]{\xi}, \sqrt[l^m]{a_i} \mid \xi \in U_K, i = 1, \dots, r)$ , where  $U_K$  is the group of units of  $K$  and  $\mathfrak{p}$  a prime of  $K$  which splits completely in  $K''$ . Then there is a cyclic  $l^m$ -extension of  $K$  that is totally ramified at  $\mathfrak{p}$  and is not ramified at any other prime of  $K$ .*

COROLLARY 3.5. *Let  $K/\mathbb{F}_p(t)$  be a function field,  $n$  a positive integer with  $(n, p) = 1$ . Then there exists a finite extension  $K'''$  of  $K$  such that if  $\mathfrak{p}$  is any prime of  $K$  that splits completely in  $K'''$ , then there exists a cyclic extension  $L/K$  of degree  $n$  in which  $\mathfrak{p}$  is totally ramified and  $\mathfrak{p}$  is the only prime of  $K$  that ramifies in  $L$ .*

*Proof.* We modify the number field case found in [?].

Let  $n = \prod_q q^{m(q)}$  be the decomposition of  $n$  into primes. Let  $K'' = K''(q)$  by taking  $m = m(q)$  in Lemma 3.4, then let  $K'''$  be the compositum of the fields  $K''(q)$ . Let  $L(q)$  be the cyclic extension of degree  $q^{m(q)}$  provided by Lemma 3.4. The compositum  $L = \prod L(q)$  has the desired property.  $\square$

THEOREM 3.6. *Let  $G$  be a finite semiabelian group, of order prime to  $p$ . Then there exists a tamely ramified extension  $K/\mathbb{F}_p(t)$  with Galois group  $G$  in which at most  $d(G)$  primes ramify.*

Note, this does not go as far as Conjecture 1.1, as we are finding  $d(G)$  not  $d(G^{ab})$  ramified primes (here  $p(G) = \{1\}$ ). However, when the two are equal, as is the case for all  $l$ -groups by Burnside's Basis Theorem [?, p. 46], we will then have shown Conjecture 1.1.

*Proof.* Again, this is a modification of the number field case found in [?]. By definition,  $G$  is a homomorphic image of  $C_1 \wr (C_2 \wr \dots \wr C_r)$ ,  $r = wl(G) = d(G)$ . Thus we may assume  $G \cong C_1 \wr (C_2 \wr \dots \wr C_r)$ . We then induct on  $r$ .

For  $r = 1$ ,  $G$  is cyclic. Then we are done by Theorem 2.6.

Now, assume the theorem holds for  $r - 1$ . Let  $K_1/\mathbb{F}_p(t)$  be a tamely ramified Galois extension with  $\text{Gal}(K_1/\mathbb{F}_p(t)) \cong C_2 \wr (C_3 \wr \dots \wr C_r)$  such that the ramified primes in  $K_1$  are a subset of  $\{q_2, \dots, q_r\}$ . By Corollary 3.5, there exists a field  $K_1'''$ , the field supplied for  $K_1$  by Corollary 3.5, and a prime  $\mathfrak{q} = \mathfrak{q}_1$  which splits completely in  $K_1'''$ . Let  $\mathfrak{p} = \mathfrak{p}_1$  be a prime of  $K_1$  dividing  $\mathfrak{q}$ . Then there exists a cyclic extension  $L/K_1$  with  $\text{Gal}(L/K_1) \cong C_1$  in which  $\mathfrak{p}$  is totally ramified and in which  $\mathfrak{p}$  is the only prime of  $K_1$  which ramifies in  $L$ .

Let  $\{\sigma(\mathfrak{p}) \mid \sigma \in \text{Gal}(K_1/\mathbb{F}_p(t))\}$  be the  $|G_1|$  distinct conjugates of  $\mathfrak{p}$  over  $K_1$ . Let  $M$  be the compositum of  $\sigma(L)$ , as  $\sigma$  runs over  $\text{Gal}(K_1/\mathbb{F}_p(t))$ . Then it follows that the fields  $\{\sigma(L) \mid \sigma \in \text{Gal}(K_1/\mathbb{F}_p(t))\}$  are linearly disjoint over  $K_1$ , and so

$$\text{Gal}(M/\mathbb{F}_p(t)) \cong C_1 \wr G_1 \cong G.$$

With the ramified primes of  $M/\mathbb{F}_p(t)$  a subset of  $\{q_1, \dots, q_r\}$ . Then  $M$  satisfies the conditions of the theorem.  $\square$

#### 4. SMALL GROUP EXAMPLES

Before we proceed further, it is useful to examine several concrete examples. In the process of proving these cases, it is advantageous to have a definitive method for determining

the ramification at the infinite prime. We use the following criterion when dealing with explicit examples:

LEMMA 4.1 (Ramification at Infinity). *Suppose  $f(x)$  has a splitting field  $K/\mathbb{F}_p(t)$ . The following procedure is sufficient to determine if the infinite prime  $(1/t)$  ramifies in the extension  $K/\mathbb{F}_p(t)$ .*

- (1) *Substitute  $xt^b$  for  $x$ .*
- (2) *Divide by  $t^{b \cdot \deg f}$ .*
- (3) *Mod out by  $1/t$  to get  $g(x)$ .*
- (4) *Determine if  $g(x)$  has a repeated root.*

Here,  $b$  is the smallest integer such that after step 2 there are no positive powers of  $t$  left.

*Proof.* We employ the first two steps to obtain a polynomial in  $1/t$  instead of  $t$ . As in [?, Lemma 3.5.3, Cor 3.5.11], we can then check the ramification by reducing mod  $1/t$ .  $\square$

One of the most useful tools we have in the function field case is an analogue of Schinzel's Hypothesis-H that allows us to produce irreducible polynomials satisfying certain properties:

THEOREM 4.2 (Pollack, [?]). *Let  $n$  be a positive integer. Let  $f_1(x), \dots, f_r(x)$  be nonassociate irreducible polynomials over  $\mathbb{F}_q$  with the degree of the product  $f_1 \cdots f_r$  bounded by  $B$ . The number of univariate monic polynomials  $g$  of degree  $n$  for which all of  $f_1(g(t)), \dots, f_r(g(t))$  are irreducible over  $\mathbb{F}_q$  is*

$$\frac{q^n}{n^r} + O_{n,B} \left( q^{n-\frac{1}{2}} \right)$$

provided  $\gcd(q, 2n) = 1$ .

Pollack gives explicit upper and lower bounds here for most  $q$ . In particular, if we let  $C$  be the number of such  $g$ , we have

$$C \geq \left( q^{n-1} - 4n^2 q^{n-2} \left( 1 + \binom{B}{2} \right) \right) \left( \frac{q}{n^r} - \frac{2}{n^r} \left( q^{1/2} + 1 + n!^B \right) - (n-1)B \right)$$

when  $q$  is sufficiently large. Specifically,  $q$  must be large enough to satisfy

$$q > 4n^2 \left( 1 + \binom{B}{2} \right).$$

Taken together, these then ensure that  $C > 0$ . Thus, when  $q$  is sufficiently large we can always find at least one such  $g$ .

With this tool in hand, we now proceed to outline several specific examples that provide support for Conjecture 1.1.

4.1.  $D_8$ . We begin with a group covered in the previous theorems (specifically Theorem 2.5 and Theorem 3.6), namely, the dihedral group of order 8. It is useful, however, to consider this group explicitly.

THEOREM 4.3. *Conjecture 1.1 holds for  $G = D_8$ , the dihedral group of order 8. Namely, there exists a  $D_8$ -extension of  $\mathbb{F}_p(t)$  ramified at exactly 2 primes (counting the infinite prime) when  $p \neq 2$ , or one prime when  $p = 2$ . Moreover, there is no such extension ramified at fewer primes.*

*Proof.* When  $p = 2$ , this falls under Theorem 2.5. We now consider the case  $p \neq 2$ .

Every dihedral extension can be defined by a polynomial of the form  $f(x) = x^4 + ax^2 + b$ . Further, any such choice of  $a, b$  will yield a dihedral extension when  $b$ ,  $a^2 - 4b$ , and  $b(a^2 - 4b)$  are all not squares. Then, the discriminant of  $f$  is

$$16b(a^2 - 4b)^2,$$

so it is sufficient to check the ramification in each each of the fields defined by  $x^2 - b$ ,  $x^2 - (a^2 - 4b)$ , and  $x^2 - b(a^2 - 4b)$ .

Now, based on the abelian theory above, it is sufficient to find  $a, b$ , with  $b$  irreducible, satisfying the non-square conditions described, and then show that the infinite prime does not ramify.

We use Lemma 4.1 to test the ramification at the infinite prime. In most cases,  $(1/t)$  will still ramify, but if  $2 \deg a = \deg b$ , and  $A^2 - 4B$  is not a square,  $f$  is unramified at infinity. Here  $A$  and  $B$  are the leading coefficients of  $a$  and  $b$ , respectively.

Choose  $a$  such that  $A^2 - 4$  is not a square. Choose  $d \in \mathbb{F}_p[t]$ , a square element. Let

$$g_1(x) = a^2 - 4x, \quad g_2(x) = x(a^2 - 4x) - d.$$

Then use Theorem 4.2 to choose a monic irreducible  $b \in \mathbb{F}_p[t]$  such that  $g_1(b)$  and  $g_2(b)$  are still irreducible. Thus, by choice of  $b$ ,  $f(x)$  must define a dihedral extension ramified at only two finite primes, and by choice of  $a$ ,  $f(x)$  is unramified at infinity. Note, Theorem 4.2 will give the existence of such a  $b$  as long as

$$p > 4n^2 \left( 1 + \binom{B}{2} \right).$$

As we may let  $n = 4$ , Theorem 4.2 then produces the desired  $b$  for  $p > 256$ . We provide explicit examples for the remaining primes in Table 1. (Note that for  $p = 3$ , we do not give an irreducible  $b$ , but instead  $b = 2(t+2)^4$ . It is not a perfect square, so the extension is still dihedral, and it is the power of a single prime, so only one prime ramifies in the extension generated by  $x^2 - b$ .)

For minimality, note that any dihedral extension has a Klein-4 subextension, and hence by the abelian theory above must have at least two primes that ramify.  $\square$

**4.2.  $S_3$ .** We now examine the symmetric group on three elements. This group, being the smallest nonabelian example, provides much direction for further work. Consider the polynomial

$$f(x) = x^3 - uwx - u^2, \quad w, u \in \mathbb{F}_p[t]$$

where  $u$  and  $w$  are relatively prime. Note, the discriminant of  $f(x)$  is  $d = 4u^3w^3 - 27u^4$ . For a field  $K$ , let  $h(K)$  denote the divisor class number, namely the order of the finite portion of the class group. Then

**THEOREM 4.4.** [?] *When  $p > 3$ , if  $d$  is not a square in  $\mathbb{F}_p(t)$ , then  $3 \mid h(\mathbb{F}_p(t)(\sqrt{d}))$ . Conversely, every quadratic function field whose divisor class number is divisible by 3 is given in this way by some  $u$  and  $w$ .*



LEMMA 4.5. *Let  $K/\mathbb{F}_p(t)$  be a quadratic extension. Then  $3|h(K)$  if and only if there exists an unramified geometric cyclic extension  $L/K$  such that  $L$  is Galois over  $\mathbb{F}_p(t)$  with Galois group isomorphic to  $S_3$ .*

*Proof.* By class field theory we have an unramified degree 3 extension of  $K$  for every quotient of order 3 of the class group. At least one of these must be Galois over  $\mathbb{F}_p(t)$ . Thus it will have Galois group  $S_3$  or  $\mathbb{Z}/6\mathbb{Z}$ . However, the latter would then yield an unramified cubic extension of  $\mathbb{F}_p(t)$  which is impossible.  $\square$

LEMMA 4.6. [?] *Consider  $f(x)$  defined above. If  $f$  is irreducible, let  $K = \mathbb{F}_p(t)(\sqrt{d})$  and  $L/\mathbb{F}_p(t)$  be the splitting field of  $f$ .  $L$  is unramified over  $K$  if and only if  $v = w^3$  and  $\deg u < \deg v$  or  $3 \mid \deg u$ .*

We will use this result to control the ramification for general  $p$ .

THEOREM 4.7. *Conjecture 1.1 holds for  $G = S_3$  and  $p \equiv 0, 1 \pmod{3}$ . Namely, there exists an  $S_3$ -extension of  $\mathbb{F}_p(t)$  ramified at only one prime. Moreover, there is no such extension ramified at fewer primes.*

*Proof.* Note, minimality is ensured by Corollary 2.7 or by Hermite's Theorem for function fields [?, Theorem III.2.16]. For existence, we consider several cases.

( $p = 2$ ) Note that  $G/p(G) \cong \{1\}$ , which has zero generators, according to our convention. Then we are expecting the minimal number of ramified primes to be 1.

TABLE 1. We present the explicit examples for small primes that have Galois group  $D_8$ . Here, we have a defining polynomial

$$f(x) = x^4 + ax^2 + b$$

We give the values of  $A$ ,  $A^2 - 4B$ ,  $a$ , and  $b$ , where  $A$  is the leading coefficient of  $a$ , and  $B$  is the leading coefficient of  $b$ .

$p$	$A$	$A^2 - 4B$	$a$	$b$	$p$	$A$	$A^2 - 4B$	$a$	$b$
3	2	2	$2t^2 + t + 1$	$2t^4 + t^3 + t + 2$	109	11	8	$11t^2 + 3$	$t^4 + 5t + 1$
5	1	2	$t^2 + 2$	$t^4 + 2$	113	32	3	$32t^2 + 3$	$t^4 + t + 1$
7	3	5	$3t^2 + 3t$	$t^4 + t + 1$	127	3	5	$3t^2 + 3$	$t^4 + 4t + 1$
11	1	8	$t^2 + 3t + 1$	$t^4 + 4t + 1$	131	55	8	$55t^2 + 6$	$t^4 + t + 1$
13	3	5	$3t^2 + 7$	$t^4 + t + 1$	137	12	3	$12t^2$	$t^4 + t + 1$
17	3	5	$3t^2$	$t^4 + 3t + 1$	139	4	12	$4t^2 + 1$	$t^4 + 3t + 1$
19	5	2	$5t^2 + 1$	$t^4 + 6t + 1$	149	4	12	$4t^2 + 1$	$t^4 + 16t + 1$
23	3	5	$3t^2 + 3$	$t^4 + 4t + 1$	151	37	6	$37t^2 + 3$	$t^4 + 5t + 1$
29	8	2	$8t^2 + 7$	$t^4 + 3t + 1$	157	3	5	$3t^2 + 1$	$t^4 + t + 1$
31	4	12	$4t^2$	$t^4 + t + 1$	163	13	2	$13t^2 + 3$	$t^4 + t + 1$
37	3	5	$3t^2 + 3$	$t^4 + 5t + 1$	167	3	5	$3t^2$	$t^4 + 3t + 1$
41	4	12	$4t^2 + 1$	$t^4 + t + 1$	173	51	2	$51t^2$	$t^4 + 7t + 1$
43	7	2	$7t^2 + 5$	$t^4 + 5t + 1$	179	38	8	$38t^2 + 1$	$t^4 + t + 1$
47	3	5	$3t^2 + 3$	$t^4 + 5t + 1$	181	83	7	$83t^2 + 3$	$t^4 + 8t + 1$
53	1	50	$t^2$	$t^4 + 3t + 1$	191	46	11	$46t^2 + 6$	$t^4 + 4t + 1$
59	1	56	$t^2$	$t^4 + t + 1$	193	3	5	$3t^2 + 8$	$t^4 + 8t + 1$
61	5	21	$5t^2$	$t^4 + 3t + 1$	197	91	3	$91t^2 + 12$	$t^4 + 11t + 1$
67	26	2	$26t^2$	$t^4 + t + 1$	199	87	3	$87t^2 + 1$	$t^4 + t + 1$
71	19	2	$19t^2 + 4$	$t^4 + 8t + 1$	211	46	2	$46t^2 + 1$	$t^4 + t + 1$
73	3	5	$3t^2$	$t^4 + 4t + 1$	223	26	3	$26t^2 + 4$	$t^4 + 13t + 1$
79	13	7	$13t^2 + 3$	$t^4 + 6t + 1$	227	3	5	$3t^2 + 6$	$t^4 + 4t + 1$
83	3	5	$3t^2 + 6$	$t^4 + 10t + 1$	229	34	7	$34t^2 + 4$	$t^4 + 21t + 1$
89	10	7	$10t^2$	$t^4 + 3t + 1$	233	3	5	$3t^2 + 7$	$t^4 + 8t + 1$
97	3	5	$3t^2 + 9$	$t^4 + 4t + 1$	239	49	7	$49t^2 + 4$	$t^4 + 5t + 1$
101	39	2	$39t^2 + 5$	$t^4 + t + 1$	241	16	11	$16t^2 + 6$	$t^4 + 11t + 1$
103	25	3	$25t^2 + 1$	$t^4 + 5t + 1$	251	99	8	$99t^2 + 8$	$t^4 + 15t + 1$
107	3	5	$3t^2 + 1$	$t^4 + 14t + 1$					

As an example of the existence of such an extension, consider the field defined by

$$f(x) = x^2 + x + (t + 1)^3.$$

Computations confirm that only the infinite prime ramifies. This field has class group  $\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ , thus there is a cubic extension of the quadratic field which is an  $S_3$ -extension over  $\mathbb{F}_p(t)$  by Lemma 4.5.

( $p = 3$ ) Note that  $G/p(G) \cong \mathbb{Z}/2\mathbb{Z}$ , which has one generator. Then we are expecting the minimal number of ramified primes to be 1.

Consider the splitting field of the polynomial

$$f(x) = x^3 - (t^2 + 1)x + (t - 1),$$

whose discriminant is  $D = (t^2 + 1)^3$ . Computations confirm that  $(t^2 + 1)$  ramifies, and that it is the only prime that ramifies in the quadratic subextension. The discriminant is not a square, thus we again retrieve an  $S_3$ -extension ramified at only one finite prime [?, p. 612].

( $p \geq 7$ ,  $p \equiv 1 \pmod{3}$ ) Note that  $(G/p(G))^{ab} \cong \mathbb{Z}/2\mathbb{Z}$ , which has one generator. Then we are expecting the minimal number of ramified primes to be 1. Let  $k = \mathbb{F}_p(t)$  and define

$$f(x) = x^3 - uwx - u^2$$

where  $u, w \in \mathbb{F}_p[t]$  are relatively prime with  $\deg u < 3 \deg w$  or  $3 \mid \deg u$ . Thus by Lemma 4.6 and Theorem 4.4 we have its splitting field is an  $S_3$ -extension with all the ramification in the quadratic subextension. Then  $f$  has discriminant

$$d = 4u^3w^3 - 27u^4 = u^3(4w^3 - 27u).$$

Suppose  $f$  is irreducible over  $k$ . Then work of Li and Zhang [?, Lemma 2.2] implies that  $K/k$  will have only one finite ramified prime if we can choose  $u, w$  such that  $u \in \mathbb{F}_p$  and  $w$ , nonconstant, such that  $\pi = 4w^3 - 27u$  is irreducible. With such a choice of  $u$  and  $w$ , it is easy to see that  $f$  is irreducible: if  $f$  factored, it would have a root in  $\mathbb{F}_p[t]$  but this would then imply that  $f$  would have a root in  $\mathbb{F}_p$ , forcing  $w \in \mathbb{F}_p$ , which is false.

By Lemma 4.1 we see that the infinite prime will always ramify if  $\deg w$  is odd. However, if  $\deg w$  is even and  $w$  is monic, we arrive at  $g(x) = x(x^2 - u)$ . This will not have a repeated root so long as we can choose  $u \neq 0$  in  $\mathbb{F}_p$ , since  $p \neq 2$ . Thus we can choose a polynomial where the infinite prime does not ramify, so we have an extension ramified at only one prime.

Now, it suffices to show that there always is such a choice of  $u$  and  $w$ , with  $\pi$  irreducible and  $w$  of even degree. For this we apply Theorem 4.2. As seen previously, it is possible to choose parameters to guarantee a nonzero answer when  $p$  is sufficiently large; in this case, when  $p > 64$  and when  $\mathbb{F}_p \neq \mathbb{F}_p^2$ ; this requires that  $p \equiv 1 \pmod{3}$ . We give explicit examples for the remaining primes in Table 2.

□

## 5. DIHEDRAL GROUPS

We now attempt to generalize the previous results. Given a finite cyclic group  $A$  with  $|A| = a$ , we can form the semidirect product  $A \rtimes \mathbb{Z}/2\mathbb{Z}$ , the dihedral group of order  $2a$ , and denote it by  $D_{2a}$ .

LEMMA 5.1. *Suppose  $p \neq 2$ . Let  $A$  be as above, with  $(a, 2) = 1$  and  $(a, p) = 1$ . Let  $K/\mathbb{F}_p(t)$  be a quadratic extension with only one ramified prime,  $N \in \mathbb{F}_p[t]$ . There exists a minimally ramified  $A$ -extension of  $K$ , call it  $L/K$ , with one ramified prime, such that  $L/\mathbb{F}_p(t)$  is Galois.*

*Proof.* Carlitz-Hayes theory as defined over  $K = \mathbb{F}_p(t)$ , can be generalized over any field assuming the embedding

$$\alpha : \text{Gal}(K(\Lambda_M)/K) \hookrightarrow (\mathbb{F}_p[t]/M)^\times$$

is an isomorphism. We refer to the proof of the above fact for  $K = \mathbb{F}_p(t)$  and the discussion of generalizations found in [?, ?, ?]. For  $M \in \mathcal{O}_K$ , define

$$\Phi(M) = |(\mathcal{O}_K/M)^\times|.$$

Choose  $M \in \mathcal{O}_K$  irreducible such that

$$\Phi(M) \equiv 0 \pmod{a(p-1)},$$

and for  $M|M'$ ,  $M' \in \mathbb{F}_p[t]$ ,

$$\Phi(M') \equiv 0 \pmod{2(p-1)}$$

but

$$\Phi(M') \not\equiv 0 \pmod{2a(p-1)}.$$

Such an  $M$  and  $M'$  exist by definition of  $\Phi$  and the fact that  $p \nmid 2, a$ . Note, the proof referenced above shows  $\text{Gal}(K(\Lambda_M)/K) \cong (\mathcal{O}_K/M)^\times$  for  $M \in \mathcal{O}_K$ , and taking the congruences with a  $p-1$  term in the modulus guarantees that infinity will not ramify [?, Theorem 3.2]. Then  $A$  is isomorphic to a quotient of  $(\mathcal{O}_K/M)^\times$  and, since by our choice  $M$  lies over a prime  $M'$  with no inertia, is isomorphic to a quotient of  $(\mathbb{F}_p[t]/M')^\times$ . So with a choice of such an  $M$ , we can build such an  $A$ -extension  $L/K$ . Further,  $L/K$  has one ramified prime by our choice of  $M$ , namely  $M$  itself.

Now, to see that  $L/\mathbb{F}_p(t)$  is Galois, it is sufficient to note that  $(\mathbb{F}_p[t]/N)^\times$  acts on  $(\mathbb{F}_p[t]/M')^\times$ . But as  $M'$  is by construction ramified in  $L/\mathbb{F}_p(t)$ , and  $N$  is the only ramified prime in  $K/\mathbb{F}_p(t)$ , our choice of  $M$  forces  $M' = N$ .  $\square$

TABLE 2. We present the explicit examples for small primes that have Galois group  $S_3$ . Here, we have a defining polynomial

$$f(x) = x^3 - uwx - u^2$$

The discriminant is then

$$d = 4u^3w^3 - 27u^4 = u^3(4w^3 - 27u)$$

We give the value of  $u$  and  $w$  for each prime, as well as the value of  $\pi = 4w^3 - 27u$ .

$p$	$u$	$w$	$\pi$
7	6	$t^2 + 3$	$4t^6 + t^4 + 3t^2 + 2$
13	2	$t^2$	$4t^6 + 11$
19	2	$t^2 + 1$	$4t^6 + 12t^4 + 12t^2 + 7$
31	3	$t^2 + 1$	$4t^6 + 12t^4 + 12t^2 + 6$
37	2	$t^2$	$4t^6 + 20$
43	3	$t^2 + 1$	$4t^6 + 12t^4 + 12t^2 + 9$
61	2	$t^2$	$4t^6 + 7$

Note, the condition that  $(a, 2) = 1$  ensures that we fall into one of two cases. If  $L/\mathbb{F}_p(t)$  is cyclic it has Galois group  $A \rtimes \mathbb{Z}/2\mathbb{Z}$  and then it could have been achieved by the Carlitz-Hayes theory shown previously and thus we only have one ramified prime, namely  $M = M'$ ; this was excluded by our choice of  $M$  and  $M'$ . If  $L/\mathbb{F}_p(t)$  is not cyclic but Galois, it has Galois group  $A \rtimes \mathbb{Z}/2\mathbb{Z} \cong D_{2a}$ , and  $M'$  is the only ramified prime. Then we have:

**THEOREM 5.2.** *Suppose  $p \neq 2$ . Let  $A$  be a cyclic group of odd prime order  $a$ ,  $p \neq a$ . Then  $D_{2a}$  satisfies Conjecture 1.1.*

*Proof.* According to our conjecture, we are expecting only one ramified prime. Construct a minimally ramified quadratic extension  $K/\mathbb{F}_p(t)$  as in Theorem 2.6. Then we use Lemma 5.1 to produce an  $A$ -extension of  $K$ , minimally ramified, giving an extension  $L/\mathbb{F}_p(t)$  having one ramified prime.

To ensure that this extension is not a cyclic extension and that only one prime ramifies, it is enough to carefully pick  $M \in \mathcal{O}_K$  and  $N \in \mathbb{F}_p[t]$  with  $M|N$  but  $M \neq N$ , as in Lemma 5.1. Then  $N$  is the only prime ramifying in  $L/\mathbb{F}_p(t)$ , but  $L/\mathbb{F}_p(t)$  cannot be cyclic. Hence we must have  $\text{Gal}(L/\mathbb{F}_p(t)) \cong A \rtimes \mathbb{Z}/2\mathbb{Z}$ , with one ramified prime. To see that this is in fact  $D_{2a}$  we note that when  $a$  is an odd prime there is only one homomorphism

$$\varphi : \mathbb{Z}/2\mathbb{Z} \hookrightarrow \text{Aut}(A)$$

and hence only one semidirect product, namely  $D_{2a}$ . □

## 6. EMBEDDING PROBLEMS

**6.1. Embedding theory.** Let  $F$  be a field and  $\overline{F}$  a separable closure of  $F$ . Then define  $G_F = \text{Gal}(\overline{F}/F)$ . A Galois extension  $N/F$  with group  $G$  is then defined by taking a surjection

$$\phi : G_F \longrightarrow G$$

and setting  $N = \overline{F}^{\ker \phi}$ . Suppose  $K/F$  is Galois with group  $G$  with associated surjection  $\phi : G_F \rightarrow G$ . Consider a group  $\tilde{G}$  with an exact sequence

$$1 \longrightarrow H \xrightarrow{\iota} \tilde{G} \xrightarrow{\kappa} G \longrightarrow 1.$$

The *embedding problem*  $\varepsilon(\phi, \kappa)$  is the question of whether there exists a homomorphism

$$\tilde{\phi} : G_F \longrightarrow \tilde{G}$$

which extends  $\phi$  via  $\kappa$  such that the following diagram commutes:

$$\begin{array}{ccccccc} & & & & G_F & & \\ & & & \tilde{\phi} \swarrow & \downarrow \phi & & \\ 1 & \longrightarrow & H & \xrightarrow{\iota} & \tilde{G} & \xrightarrow{\kappa} & G \longrightarrow 1. \end{array}$$

If  $\tilde{\phi}$  is surjective, we say it is a *proper* solution. Then the corresponding field  $\tilde{N} := \overline{F}^{\ker \tilde{\phi}}$  is a  $\tilde{G}$ -extension of  $F$ . We call  $H$  the *kernel* of the embedding problem  $\varepsilon(\phi, \kappa)$ . We call  $\varepsilon(\phi, \kappa)$  *finite* if  $\tilde{G}$  is a finite group, *split* if the group extension  $\tilde{G} = H \cdot G$  splits, *central*

if  $H$  lies in the center of  $\tilde{G}$ , and *Frattini* if  $H$  lies in the Frattini subgroup of  $\tilde{G}$ . In the case where  $F$  is a function field with field, we call  $\varepsilon(\phi, \kappa)$  a *geometric embedding problem* if  $N := \overline{F}^{\ker \phi}$  is geometric over  $F$ , or equivalently regular over the field of constants of  $F$ .

It is possible to break embedding problems up into smaller pieces as follows:

**THEOREM 6.1** (Dentzer, [?]). *Let the kernel  $H$  of an embedding problem  $\varepsilon(\phi, \kappa)$  have a decomposition  $H = H_1 \times H_2$  as a direct product of normal subgroups of  $\tilde{G}$ . For  $\tilde{G}_1 = \tilde{G}/H_1$  and  $\tilde{G}_2 = \tilde{G}/H_2$ , and the induced epimorphism  $\kappa_i : \tilde{G}_i \rightarrow \text{Gal}(N/F)$  the following hold:*

- *The embedding problem  $\varepsilon(\phi, \kappa)$  is solvable if and only if the embedding problems  $\varepsilon(\phi, \kappa_i)$  are solvable. For the corresponding solution fields,  $\tilde{N} = \tilde{N}_1 \tilde{N}_2$  holds.*
- *$\varepsilon(\phi, \kappa)$  possesses a proper solution if and only if  $\varepsilon(\phi, \kappa_i)$  have proper solutions  $\tilde{N}_1, \tilde{N}_2$  that are linearly disjoint over  $N$ .*
- *Let  $F$  be a function field over  $k$ . If  $\varepsilon(\phi, \kappa)$  possesses a geometric solution, then so do  $\varepsilon(\phi, \kappa_i)$ . If these have geometric solutions  $\tilde{N}_1$  and  $\tilde{N}_2$  such that the fields  $\overline{k}\tilde{N}_i$  are linearly disjoint over  $\overline{k}F$ , then  $\varepsilon(\phi, \kappa)$  also has a geometric solution.*

Further, we have

**THEOREM 6.2** (Dentzer, [?]). *Let  $F$  be a Hilbertian field and  $H$  a finite group, being the Galois group of a geometric extension of the rational function field  $F(x)$ . Further let  $K$  be a finite Galois extension of  $F$  with group  $G$  and let  $\tilde{G}$  be one of the following extensions of  $G$ :*

- $\tilde{G} = G \times H$
- $\tilde{G} = G \wr H$
- *Let  $H$  be abelian and  $\tilde{G} = G \ltimes H$*

*Let  $K$  be the corresponding projection in each case. Then the embedding problem  $\varepsilon(\phi, \kappa)$  possesses a proper solution. If  $F = k(t)$  is a rational function field and  $K$  is a geometric extension of  $F$ , then there exists even a proper geometric solution.*

Define

$$\text{Ram}(L/K) = \{\mathfrak{p} \in \mathbb{P}(K) \mid \mathfrak{p} \text{ ramifies in } L/K\}.$$

A finite Galois extension  $N/F$  is called an *n-Scholz extension* if all  $\mathfrak{p} \in \text{Ram}(N/F)$  and  $\tilde{\mathfrak{p}}$  lying over  $\mathfrak{p}$  satisfy  $\zeta_n \in F_{\tilde{\mathfrak{p}}}$  and  $D(\tilde{\mathfrak{p}}/\mathfrak{p}) = I(\tilde{\mathfrak{p}}/\mathfrak{p})$ . We call  $\varepsilon(\phi, \kappa)$  an *n-Scholz embedding problem* if the fixed field  $N$  of  $\ker(\phi)$  is an *n-Scholz extension* of  $F$  and a solution  $\tilde{\phi}$  an *n-Scholz solution* if the solution field  $\tilde{N}$  is an *n-Scholz extension* of  $K$  [?, Chap 4]. We define the *socle* of a Galois  $l$ -extension  $N/F$  with group  $G$  to be the maximal elementary abelian intermediate field. In other words, the fixed field of  $\Phi(G) = G^l G'$ .

**6.2. General  $l$ -groups.** Recall that all finite  $l$ -groups have an upper central series of the form

$$1 = G_0 \leq G_1 \leq \cdots \leq G_n = G$$

with each  $G_{i+1}/G_i \cong \mathbb{Z}/l\mathbb{Z}$ .

**PROPOSITION 6.3.** [?, p. 358] *Let  $(l, p-1) \neq 1$  and  $G$  a finite  $l$ -group with  $d(G^{ab}) = s$ . Then for each  $\mathbb{T}$  as in Lemma IV.10.10 [?, p. 358], of which there are infinitely many, there*

exists a geometric Galois extension  $N/\mathbb{F}_p(t)$  with

$$\mathrm{Gal}(N/\mathbb{F}_p(t)) \cong G$$

and

$$\mathrm{Ram}(N/\mathbb{F}_p(t)) = \{\tilde{\mathfrak{q}}_1, \dots, \tilde{\mathfrak{q}}_s\},$$

where each  $\tilde{\mathfrak{q}}_i \in \mathbb{P}(\mathbb{F}_p(t))$  are the uniquely determined extensions of  $\mathfrak{q}_i \in \mathbb{T}$ .

COROLLARY 6.4. *Let  $(l, p-1) \neq 1$ . Then every finite  $l$ -group satisfies Conjecture 1.1.*

*Proof.* Existence is based on Proposition 6.3, and minimality follows from Corollary 2.7.  $\square$

LEMMA 6.5. [?, p. 353] *Let  $K = \mathbb{F}_p(t)$ ,  $l \neq p$  a prime with  $(l, p-1) = 1$ , and  $\mathbb{S} \subset \mathbb{P}(K)$  a finite subset. Then we have:*

- (1) *Every split central (geometric)  $l^m$ -Scholz embedding problem  $\varepsilon(\phi, \kappa)$  over  $K$  with kernel  $\mathbb{Z}/l\mathbb{Z}$  and  $\exp_l(\phi(G_K)) < l^m$  possesses a proper (geometric)  $l^m$ -Scholz solution.*
- (2) *If  $\phi(G_K)$  is an  $l$ -Group and the socle of  $N/K$  of the fixed field  $N$  of  $\phi(G_K)$  is unramified outside of  $\mathbb{S}$  only, then  $\varepsilon(\phi, \kappa)$  possesses also such a solution. Moreover, its solution field  $\tilde{N}$  satisfies*

$$\mathrm{Ram}(\tilde{N}/K) \subseteq \mathrm{Ram}(N/K) \cup \{\mathfrak{q}\}$$

for some  $\mathfrak{q} \in \mathbb{P}(K) \setminus \mathbb{S}$ .

Note, the choice of  $\mathfrak{q}$  guarantees the new extension will also be Scholz.

LEMMA 6.6. [?, p. 354] *Let  $K$  and  $\mathbb{S}$  be as in 6.5. Then every (geometric) non-split central  $l^m$ -Scholz embedding problem  $\varepsilon(\phi, \kappa)$  over  $K$  with kernel  $\mathbb{Z}/l\mathbb{Z}$  and  $\exp_l(\phi(G_K)) < l^m$  possesses a proper (geometric) solution, where the solution field  $\tilde{N}$  satisfies*

$$\mathrm{Ram}(\tilde{N}/K) = \mathrm{Ram}(N/K).$$

LEMMA 6.7. *Let  $K$  and  $\mathbb{S}$  be as in 6.5. Then every (geometric) non-split central  $l^m$ -Scholz embedding problem  $\varepsilon(\phi, \kappa)$  over  $K$  with kernel  $\mathbb{Z}/l\mathbb{Z}$  and  $|\phi(G_K)| = l^n < l^m$  possesses a proper (geometric)  $l^m$ -Scholz solution, where the solution field  $\tilde{N}$  satisfies*

$$\mathrm{Ram}(\tilde{N}/K) = \mathrm{Ram}(N/K).$$

*Proof.* By Lemma 6.6 we already have a proper solution  $\tilde{\phi}$  whose solution field  $\tilde{N}$  satisfies the requisite ramification condition. We will modify this solution to obtain a Scholz solution.

For  $\mathfrak{r} \in \mathbb{T} := \mathrm{Ram}(\tilde{N}/K)$  with associated prime element  $r$ , fix prime divisors  $\mathfrak{R} \in \mathbb{P}(N)$  and  $\tilde{\mathfrak{R}} \in \mathbb{P}(\tilde{N})$ . Since  $I(\mathfrak{R}/\mathfrak{r}) = D(\mathfrak{R}/\mathfrak{r})$  and  $\ker \phi \cong \mathbb{Z}/l\mathbb{Z}$ , the decomposition group  $D(\tilde{\mathfrak{R}}/\mathfrak{r})$  is contained in the preimage  $\tilde{I}$  of type  $\mathbb{Z}/l\mathbb{Z} \cdot I(\mathfrak{R}/\mathfrak{r})$  in  $\tilde{G}$ . Thus it remains to show that  $\tilde{I}$  is cyclic.

By Proposition IV.10.3 [?, p. 351]

$$\tilde{G} \cong D(\tilde{\mathfrak{R}}/\mathfrak{r})$$

which is cyclic in the non-split case. Note, this is in fact a Frattini embedding problem, thus the socle remains the same.  $\square$

**COROLLARY 6.8.** *Let  $l$  be a prime with  $(l, p-1) = 1$ . Then every  $l$ -group satisfies Conjecture 1.1.*

*Proof.* Minimality follows from Corollary 2.7. For existence, we start with a cyclic extension ramified at one prime where we choose  $M \in \mathbb{F}_p[t]$  such that

$$\Phi(M) \equiv 0 \pmod{(p-1)l}$$

and thus also

$$\Phi(M) \equiv 0 \pmod{(p-1)l^m}$$

where  $m$  is such that  $|G| = l^n < l^m$  and  $\deg(M) = d$  such that  $l^m | (p^d - 1)$ . This guarantees that the base extension is Scholz. Then using the decomposition for  $l$ -groups given above, and Lemma 6.7 we produce the desired extension by induction.  $\square$

### 6.3. Nilpotent groups.

**THEOREM 6.9.** *Let  $G$  be a nilpotent group. Then  $G$  satisfies Conjecture 1.1.*

*Proof.*  $G$  is the direct product of its (unique) Sylow subgroups, thus the result follows by taking the compositum of the corresponding  $G_l$ -extensions found in Corollary 6.8 and Proposition 6.3 and the  $G_p$ -extension found in Theorem 2.5. To ensure proper ramification, start with the abelianization of  $G$  as found in Theorem 2.6 and use the cyclic subgroups of this as the starting point for the construction of each  $l$ -group.  $\square$

## 7. CONCLUSION

We have presented Conjecture 1.1 describing the expected minimal ramification for  $G$ -extensions over the field  $\mathbb{F}_p(t)$ . As evidence for this conjecture, we have established the cases where  $G$  is a  $p$ -group (Theorem 2.5), abelian (Theorem 2.6), semiabelian with  $d(G) = d(G^{ab})$  (Theorem 3.6), is dihedral of order  $2a$  where  $p \neq 2, a$  and  $a$  is an odd prime (Theorem 5.2), or is the symmetric group  $S_3$  with  $p \equiv 0, 1 \pmod{3}$  (Theorem 4.7). We then showed the case where  $G$  is an  $l$ -group,  $l \neq p$  (Corollaries 6.4 and 6.8), and used this to prove the case of Nilpotent groups (Theorem 6.9). We used methods ranging from generic polynomials and explicit computation, to the theory of pro- $p$  groups, to the theory of Drinfeld modules, to embedding theory. These examples also illustrate several different ways of piecing together new cases from those already known.

These examples, together with the previous work mentioned, lead us to believe that Conjecture 1.1 will hold true in general. Further, Boston and Markin [?] implies that we should be able to achieve a quantitative result describing how often these so-called minimal extensions appear among all  $G$ -extensions.

MEGHAN DE WITT, BRIGHAM YOUNG UNIVERSITY, PROVO, UT 84602, USA.

*E-mail address:* `megdewitt@gmail.com`

*E-mail address:* `dewitt@math.byu.edu`